UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,658	08/30/2001	Carol Lee Hobson	40655.4400	3216

7590 02/14/2006

Thomas J. Finn
Snell & Wilmer L.L.P.
One Arizona Center
400 East Van Buren
Phoenix, AZ 85004-2202

EXAMINER	
HEWITT II, CALVIN L	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 02/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/943,658	HOBSON ET AL.	
	Examiner	Art Unit	
	Calvin L. Hewitt II	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *18-25 and 35-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *18-25 and 35-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Status of Claims

1. Claims 18-25 and 35-37 have been examined.

Response to Amendment

2. Applicant is of the opinion that the prior art fails to teach Applicant's claimed method because Payne et al. do not use "... a hash to facilitate the secure submission of a payment request or the use of a hash to identify a transaction account to be charged in a transaction" (Remark, 12-20-05, page 9, first full paragraph). However, the Examiner does not find this language in the claims. Specifically, Applicant's claims, and Specification, are silent using a hash to secure a transaction. Payne et al. teach a user making a payment using a secondary transaction number (column 7, lines 22-30). The second transaction number is not money, therefore, in order to receive actual funds the merchant, or an online analog, initiates a settlement transaction using the transaction number used as a stand in for payment. A process that is old and well known to those of ordinary skill in credit card processing. Therefore, Payne et al. at least suggests "communicating said second transaction number over said authenticated communication channel to said merchant, wherein said merchant submits a payment request based on said secondary transaction account number". Payne

et al. also teach a user receiving from a host system account information including a secondary transaction number and using the secondary transaction number and the account information to facilitate a transaction (column 7, lines 22-30) (note: according to claim 23, the secondary transaction number is a part of the account information, therefore if the number is used to facilitate a transaction, the account information necessarily does).

Applicant's Specification as originally filed equates a signed challenge string with a digital certificate ("A signed challenge string (e.g., digital certificate)..." – Specification, paragraph [0054]). Therefore, attempts by the Applicant to disassociate the two by amendment are improper and subject to "new matter' rejections.

The following assertion of facts have gone unchallenged by the Applicant and are now considered admitted prior art:

- payment settlement for credit card transactions
- challenge-response protocol wherein a party A sends an encrypted (by the public key of B) random string (e.g. token) to a party B, B decrypts the string and returns the random string and a second string to A encrypted using the public key of A, A decrypts the message, verifies the first random string and if valid sends the decrypted second string back to B, thus confirming the identity of A as the original sender of the token

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 35-37 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Claim 35 recites, "wherein said challenge string and digital certificate are distinct from each other". Applicant argues that the Specification supports a signed challenge string and a digital certificate as distinct data (paragraphs 12, 34, 35, 54 and 57). However, this contradicts the clear teachings of paragraph 54, where Applicant equates the two, or at least requires one be an instance of the other (A signed challenge string (e.g., digital certificate)) (see also figure 2b, item 427). The Specification is also silent regarding some sort of comparison (paragraphs 12, 34, 35, 54 and 57). Therefore, to one of ordinary skill the Specification is unclear as to the exact relationship between the certificate and the signed challenge string.

Claims 36 and 37 are also rejected as they depend from claim 35.

5. Claims 35-37 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Based on Applicant's Disclosure, Applicant provides an embodiment where security is implemented using an authenticated communication channel (paragraph 54). In this embodiment Applicant equates a digital certificate is a with a signed challenge string (paragraph 54, figure 2b, item 427). In response, to Examiner's rejection of claim 35, Applicant has amended the Specification to recite passing the signed string and certificate to a merchant. However, this is new matter as the original presentation, in the context of online transactions using an authenticated communication channel, did not previously denote a digital certificate and a singed string as separate objects.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 35-37 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 35 recites, "comparing said signed challenge string and said digital certificate". Applicant argues that the challenge string and digital certificate are distinct data (paragraphs 12, 34, 35, 54 and 57). However, this contradicts the clear teachings of paragraph 54, where Applicant equates the two, or at least requires one be an instance of the other (A signed challenge string (e.g., digital certificate)). While, the Applicant provides multiple embodiments, this refers only to the configuration of the system such as a merchant maintaining control of a user's browser (paragraph [0054]) and not to the data exchanged. The Specification is also silent regarding some sort of comparison, therefore in order to be considered distinct, the claim should include language such as, "not one in the same" or "different".

Claims 36 and 37 are also rejected as they depend from claim 35.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314 in view of Purpura, U.S. Patent No. 6,421,768.

As per claims 18-20, Payne et al. teach an online transaction system comprising:

- receiving at a host website (payment computer) an HTTP request from a user browser (column 5, lines 25-30; column/line 9/50-10/20)
- sending said user a challenge string (column 6, lines 30-42) and authenticating said user by receiving authentication information from said user wherein the information corresponds to the user account (column 6, lines 30-59)
- generating a secondary transaction number associated with a user account and using the number to facilitate a transaction between merchant and user (column 7, lines 22-30)
- establishing an authenticated communication channel between the host and a merchant (column 7, lines 30-40)

Payne et al. disclose a host computer sending a secondary transaction number to a user and the user in turn providing the second number as payment for obtaining goods and services from the merchant (column 7, lines 15-39).

Payment "settlement" is old and well known. Therefore, it would have been obvious to one of ordinary skill for a merchant to use the payment vehicle (e.g. second transaction number) in order to collect payment (i.e. merchant submitting a payment request). Regarding the confirmation of by a merchant that a host has issued a token, Payne et al. teach a cryptographic key that is shared between host and merchant (column/line 7/65-8/2). A well-known method for securely exchanging data, such as a shared cryptographic key, is for two parties to authenticate each other's identity using a challenge-response protocol. In one such protocol, a party A sends an encrypted (by the public key of B) random string (e.g. token) to a party B, B decrypts the string and returns the random string and a second string to A encrypted using the public key of A. A decrypts the message, verifies the first random string and if valid sends the decrypted second string back to B, thus confirming the identity of A as the original sender of the token. Payne et al. also teach communicating [claims 23-25] with a user over a distributed network (figure 1), recognizing the presence of an authentication device on a user's computer system (figures 1, 4, 7 and 8; column 4, lines 35-37; column 7, lines 31-39; column 8, lines 33-38) and receiving account information from a host system to facilitate a transaction between merchant and user (column 7, lines 22-30). Payne et al. do not specifically recite a merchant redirecting a user to a host site. Purpura provides a general teaching for redirecting a user from a one computer to another over the internet (column 4,

lines 46-48 and 50-55). Purpura also discloses standard techniques for establishing an "authenticated" channel between computers. For example, Purpura discloses basic key or token exchange protocols (e.g. Interlock Protocol, Challenge-response using public key decryption) where a receiving party confirms the origination of a sent token (e.g. key) (column 4, lines 7-16). More integral to Purpura's invention, however, is an authentication protocol using basic "redirection". Specifically, Purpura teaches a first computer depositing a host system signature in a user browser and a second computer decrypting the signature to authenticate the first computer or host system (column/line 3/60-4/6). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Payne et al. and Purpura in order to allow a user authenticated on a first computer (e.g. via password- '768, column 3, lines 15-36; '314, figure 7) to be securely authenticated on a second site without having the user re-authenticate her/himself ('768, column 3, lines 38-43).

10. Claims 21-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314 and Purpura, U.S. Patent No. 6,421,768 as applied to claim 21 above, and further in view of Gifford, U.S. Patent No. 5,724,424.

As per claims 21-25, Payne et al. teach a secure online transaction system between user, merchant and host comprising password strings,

authenticated channels, and transaction numbers (abstract; figure 1; column 5, lines 25-30; column 7, lines 20-40; column/line 9/50-10/20). Purpura provides a general teaching for redirecting a user from a one computer to another over the internet (column 4, lines 46-48 and 50-55). Purpura also discloses standard techniques for establishing an "authenticated" channel between computers (column 4, lines 7-16). Purpura provides a general teaching for redirecting a user from a one computer to another over the internet (column 4, lines 46-48 and 50-55). Purpura also discloses standard techniques for establishing an "authenticated" channel between computers. For example, Purpura discloses basic key or token exchange protocols (e.g. Interlock Protocol) where a receiving party confirms the origination of a sent token (e.g. key) (column 4, lines 7-16). More integral to Purpura's invention, however, is an authentication protocol using basic "redirection". Specifically, Purpura teaches a first computer depositing a host system signature in a user browser and a second computer decrypting the signature to authenticate the first computer or host system (column/line 3/60-4/6). However, neither Payne et al. nor Purpura explicitly recite smart cards. Gifford teaches entering a personal identification number and inserting a smart card into a smart card reader (figure 4; column/line 10/54-11/8). The Gifford system authenticates users by receiving user authentication information such as a signed challenge string (e.g. digital certificate) (column 10, lines 30-53). Gifford also authenticates users based on data extracted from a payment instrument by

said authentication device (column 8, lines 1-7 and 24-31; column 10, lines 50-67). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Payne et al., Purpura and Gifford in order more securely convey private data ('314, figure 2E, items 77 and 79; column 6, lines 30-59; '424, column/line 10/54-11/8).

11. Claims 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314 in view of Gifford, U.S. Patent No. 5,724,424.

As per claims 35-37, Payne et al. teach an online transaction system comprising:

- receiving at a host website (payment computer) an HTTP request from a user browser (column 5, lines 25-30; column/line 9/50-10/20)
- sending said user a challenge string (column 6, lines 30-42) and authenticating said user by receiving authentication information from said user wherein the information corresponds to the user account (column 6, lines 30-59)
- generating a secondary transaction number associated with a user account and using the number to facilitate a transaction between merchant and user (column 7, lines 22-30)

- establishing an authenticated communication channel between the host and a merchant (column 7, lines 30-40)

Payne et al. also teach communicating [claims 23-25] with a user over a distributed network (figure 1), recognizing the presence of an authentication device on a user's computer system (figures 1, 4, 7 and 8; column 4, lines 35-37; column 7, lines 31-39; column 8, lines 33-38) and receiving account information from a host system to facilitate a transaction between merchant and user (column 7, lines 22-30). However, Payne et al. do not specifically recite retrieving from a merchant a signed challenge string and a digital certificate. Gifford teaches entering a personal identification number and inserting a smart card into a smart card reader (figure 4; column/line 10/54-11/8). Gifford also teaches authenticating users by receiving user authentication information such as a signed challenge string (e.g. digital certificate) (column 10, lines 30-53) and settlement using account numbers (figure 4; column 8,lines 17-20; column 10, lines 9-20). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Payne et al., and Gifford in order more securely convey private data ('314, figure 2E, items 77 and 79; column 6, lines 30-59; '424, column/line 10/54-11/8).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Linehan discloses a payment authentication and authorization method using signed challenge response, signed tokens, and smart cards, and payment settlement (figure 3; column 8,lines 8-15)
- Handbook of Applied Cryptography, by Menezes et al. disclose challenge and response protocols

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the date of this final action.

14. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, James P. Trammell, can be reached at (571) 272-6712.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

c/o Technology Center 3600

Washington, D.C. 20231

or faxed to:

(571) 273-8300 (for formal communications intended for entry and after-final communications),

or:

(571) 273-6709 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Calvin Loyd Hewitt II

February 6, 2006